REMARKS[1]

In the outstanding Office Action, the Examiner rejected claims 1-4 and 6-9 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,673,319 to Bellare et al. ("Bellare"). No claims are amended herein, and claims 1-4 and 6-9 remain pending.

Applicants respectfully traverse the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b) because Bellare, as relied on by the Examiner, does not anticipate claims 1-4 and 6-9.

Claim 1, for example, recites a data storage device including an encryption means for creating encrypted keys by "executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode using a storage key stored in said data storage device." Bellare fails to teach at least the claimed encryption means.

The Examiner asserts that "Bellare discloses that the first (secret) key (stored in [a] storage device) and an initialization vector are used to generate a CBC message authentication code (MAC) (Column 5 lines 5-21)." Office Action, page 3. The Examiner has thus apparently construed that the first key of Bellare corresponds to Applicants' claimed "storage key." Even if the Examiner's assertion could be considered correct, Bellare teaches:

> [i]t is assumed that the encrypting party and the decrypting party share a pair of secret keys (i.e. a first and a second key). At step 70, the plaintext string is cipher block chained using the first (secret) key and a null initialization vector (IV) to generate a CBC message authentication code (MAC) that is the (entire) last block of ciphertext. At step 72, the plaintext string is again cipher block chained, now using the second (secret) key and the CBC-MAC (generated in step 70) as the initialization vector, to thereby generate an

1 The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement of characterization in the Office Action.

> enciphered string. At step 74, the CBC-MAC (generated in step 70) and a portion of the enciphered string (generated in step 72) are then combined to create the ciphertext. Bellare, col. 5, lines 7-19 (emphasis added).

That is, a plaintext string is first cipher block chained using the first key, and the same plaintext string is cipher block chained again using the second key.

Claim 1, however, recites "executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode using a storage key" (emphasis added). That is, "the first and second set of keys" are encrypted "in a cipher block chaining (CBC) mode using a storage key." Bellare, to the contrary, can best be characterized as teaching encrypting, using cipher block chaining, a plaintext string twice, using first and second keys. Bellare provides no teaching, however, of encrypting a key, and thus also provides no teaching of encrypting "the first and second set of keys," as recited in claim 1.

Because Bellare fails to teach each and every element recited in independent claim 1, Bellare does not anticipate independent claim 1. Accordingly, Applicants respectfully submit that independent claim 1 is allowable over Bellare, and claims 2-4 are allowable at least due to their dependence on claim 1.

Claims 6-9, while of different scope, recite elements similar to those recited in independent claim 1. For example, claim 6 recites a data recording method including "encryption processing in the CBC mode on a first set of keys applicable to encryption processing on pieces of data to be stored in the sectors and a second set of keys correlating to integrity-check-value generating keys of data to be stored in at least one of the sectors." Claim 7 recites a data playback method including "executing encryption processing in the CBC mode using a storage key unique to said data storage device on

an integrity-check-value generating key of data to be stored in at least one of the sectors." Claim 8 recites a program providing medium including a computer program for "encryption processing in the CBC mode on a first set of keys applicable to encryption processing on pieces of data to be stored in the sectors and a second set of keys correlated with integrity-check-value generating keys of data to be stored in at least one of the sectors." Claim 9 recites a program providing medium including a computer program for "a set of storage-key-used CBC-mode-processing keys which is included in the header information of data stored in said data storage area and which is generated by executing encryption processing in the CBC mode using a storage key unique to said data storage device on an integrity-check-value generating key of data to be stored in at least one of the sectors." For at least the reasons given above with respect to claim 1, Applicants submit that claims 6-9 are also allowable over Bellare. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b).

In view of the foregoing remarks, Applicants submit that this claimed invention, as amended, is neither anticipated nor rendered obvious in view of the prior art reference cited against this application. Applicants therefore request the entry of this Amendment, the Examiner's reconsideration of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: October 2, 2006

By: _____
Darrell D. Kinder, Jr.
Reg. No. 57,460